Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 47 (2015) 486 – 490

Procedia Computer Science

NOVEL PRIVACY PRESERVING TECHNIQUE USING SOFT ENIGMA

R.VidyaBanu[a], N.Nagaveni[b], C.M. Ananth[c],

a Asst. Professor, Computer Applications, Sri Krishna college of Engineering and Technology,Kuniyamuthur, Coimbatore- 641008, India

b Associate Professor, Mathematics,,Coimbatore Institute of Technology, Coimbatore- 641014

c MSc SE, Sri Krishna college of Engineering and Technology, Kuniyamuthur, Coimbatore- 641008, India

Abstract

With the increased digitization of the society, more and more information about the physical world and citizens is collected and stored in databases. The collection of information by governments and corporations has created massive opportunities for knowledge-based decision making. Unfortunately, collecting huge volume of data and applying analytics also implicate privacy violations. This study is to solve the problem of security on highly confidential message passing using Soft Enigma. The main implementation of soft enigma is that by combining the concept of enigma with time variant random number. The results arrived were significant and this technique ensures highly secured message passing. This technique can be used for giving the confidential data to third party for mining purposes.

Peer-review under responsibility of organizing committee of the Graph Algorithms, High Performance Implementations and Applications (ICGHIA2014)

Keywords:

1. Introduction

Today security concerns are on the rise in all areas such as banks, governmental applications, healthcare industry, military organization, educational institutions, etc. Government organizations are setting standards, passing laws and forcing organizations and agencies to comply with these standards with

*Coresponding Author Email:vidhyabanu@yahoo.com

Peer-review under responsibility of organizing committee of the Graph Algorithms, High Performance Implementations and Applications (ICGHIA2014)
doi:10.1016/j.procs.2015.03.233

non-compliance being met with wide-ranging consequences. There are several issues when it comes to security concerns in these numerous and varying industries with one common weak link being passwords and confidential statements. Most systems today rely on security in confidential messages. However, such messages come with major management security concerns. Users tend to use easy-to-guess statements, use the same in multiple accounts, write the message or store them on their machines, etc. Furthermore, hackers have the option of using many techniques to steal passwords such as shoulder surfing, snooping, sniffing, guessing, etc. Several proper strategies for u sensitive data have been proposed. But they didn't meet the company's security concerns.

Many recent papers on privacy have focused on the perturbation model and its variants. Methods for inference attacks in the context of the perturbation model have been discussed in literature. Software-based security solutions encrypt the data to prevent data from being stolen. However, a malicious program or a hacker may corrupt the data in order to make it unrecoverable, making the system unusable. Hardware-based security solutions can prevent read and write access to data and hence offers very strong protection against tampering and unauthorized access. Hardware-based or assisted computer security offers an alternative to software-only computer security. Security tokens may be more secure due to the physical access required in order to be compromised. Access is enabled only when the token is connected and correct PIN is entered (see two-factor authentication). However, dongles can be used by anyone who can gain physical access to it. Newer technologies in hardware-based security solve this problem offering fool proof security for data. To generate the dynamic password using the personal information of the card holder and the current date, day, time and is send to the customer and the key is valid for the short duration of three minutes. Firewall is a type of security system that creates a wall that checks all incoming and outgoing messages to ensure only authorized traffic goes through. There are many different forms of this application such as Norton and Windows Security Essentials. Another way to protect your information is encryption. Encryption basically scrambles and makes any message sent unreadable to anyone who does not have a key. The key is then used to decrypt the scrambled message into the original format. One such security feature is the Soft Enigma.

2. Related Work

The basic idea of privacy preserving data mining is to develop algorithms that modify the original data in some way such that the private data and knowledge remain private even after mining process. In 1996, Clifton et al[1].analyzed that data mining can bring about threat against databases and addressed possible s olutions to achieve privacy protection of data mining. The problem of privacy-preserving data mining has found considerable attention in recent years because of recent concerns on the privacy of underlying data[2].Privacy can viewed as a social and cultural concept, and now with the emergence of web, privacy has become an issue of serious concern. Many recent papers on privacy have focused on the perturbation model and its variants. Methods for inference attacks in the context of the perturbation model have been discussed in[3]. Sweeney [4] introduced the k-anonymity privacy requirement, which requires each record in an anonymized table to be indistinguishable with at least k-1 other records within the data set, with respect to a set of quasi-identifier attributes. Vidyabanu et al. have discussed an array of perturbation based techniques for preserving the privacy of data used for clustering analysis[5,6 and 7].The usual scheme of pseudo generated random number in parallel machines is to use one and the same every process with different initial seeds[8].computer generated random numbers is, of course, that they are not truly random. For most research purposes, we rely on pseudorandom numbers generated deterministically by various mathematical algorithms[9]. The many applications of randomness have led to the development of several different methods for generating random data. Mathematicians have long known that random number generation is too important to be left to chance [10]. This, of course, is far from the truth since the scientific literature has many examples of invalid simulation results caused by bad RNGs [11]. Moreover, studies such as [12, 13 and14] have per-formed tests exposing problems in the RNGs of various popular programs offering statistical and econometric functionality. Because of the mechanical nature of these techniques, generating large numbers of sufficiently random numbers (important in statistics) required a lot of work and/or time.

There are two techniques for converting data into non readable form: Transposition technique and Substitution technique[15]. However, carefully designed cryptographically secure computationally based methods of generating random numbers do exist, such as those based on the a good deal of research has gone into pseudo-random number theory, and modern algorithms for generating pseudo-random numbers

are so good that the numbers look exactly like they were really random. Enigma featured the major operational convenience of being symmetrical (or self-inverse). This meant that decipherment worked in the same way as encipherment, so that when the cipher text was typed in, the sequence of lamps that yielded the plaintext.We have we have developed a traditional or character oriented Polyalphabetic cipher by using a simple algebraic equation[16]. It is mainly used at the time of world wars for the safe message transfer from one place to another by converting them into cipher couldn't be read by others. It is known to be one of the hard encryption techniques. a cipher text is generated which is close to the ideal line so that we have the frequencies of all alphabets equal or very close to each other then it would be impossible for an attacker to proceed with the frequency attack[17]. Transposition ciphers are stronger than simple substitution ciphers[18].

3. Enigma Based Security Mechanism

The soft enigma architecture consist of three basic elements, they are

- Plain Text (confidential message).
- Soft Enigma.
- Cipher Text.

These elements are used up in several phases of the architecture of soft enigma. Each phase of the architecture is more predominant without which soft enigma is not possible to construct. Each phase have its own unique functionality. The order of setting each phase plays a vital role in development of soft enigma

3.1 System Design

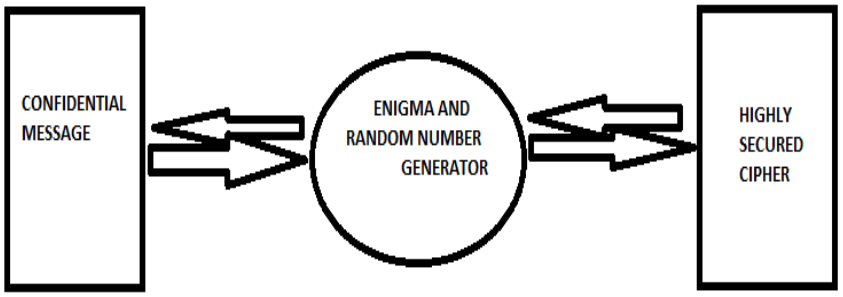

Fig. 1.Architecture

3.2 Key setting phase

Identical setting of the machines at the transmitting and receiving ends was achieved by key setting procedures. The random number generated by means of time variant is set as the key for the encryption. When the partial cipher text is generate the binary value of the key and the ciphered data is summed up. The binary key is transposition with the full cipher in order to make undifferentiated .This prevents the unauthorized user to read the message.

3.3 Message phase

The original message consists of plain text .These plain text is taken for encryption. The plain can be a character or numeric values or alphanumeric, whatever the data type of the message it can encrypted in soft enigma.

3.4 Working Phase

A good deal of research has gone into pseudo-random number theory and modern algorithms for generating pseudo-random. The additional feature that is been added to it is the concept of Enigma. This is a cryptographic device used for encryption and decryption of data. The main implementation of soft enigma

is that by combining the concept of enigma with time variant random number**.** The original message consists of plain text. The plain text is taken for encryption. The plain can be a character or numeric values or alphanumeric, whatever the data type of the message it can encrypted in soft enigma which is called as partial encryption. The time variant random number is generated and it is added with the partially encrypted data .The random number generated is the key that is to be transposition to form full cipher and send to the receiver. The full cipher consists of key and the partial cipher text. Once the fully ciphered data is received, the receiver transposes the key back and it is subtracted to get the partial the message. Using the reverse computations the original plain text is retrieved back.

4. **Performance Analysis**

The proposed mechanism is compared with the conventional DES-EEE3, Phool Proof and the results are analysed. The results show that the proposed algorithm out performs the conventional algorithms in terms of security of data, Anti key logger and key reuse.

Table 1.Performance Analysis Table.

Protocols	Security Of Data	Anti- Key Logger	Key Reuse
Soft Enigma	Yes	Yes	Yes
DES-EEE3	Yes	Yes	No
Phool Proof	Yes	No	No

4.1 Factors of Security in Soft Enigma

Security on data

The data is highly encrypted and decrypted, if any of intruder tries to change the data content it can be easily identified since the key value does not matches while decrypting the data.

Integrity

It ensures that the data it contains is valid. Data integrity means that data is protected from deletion and corruption, both while it resides within the database, and while it is being transmitted over the network. Integrity has several aspects:

- A database must be protected against viruses designed to corrupt the data.
- The network traffic must be protected from deletion, corruption, and eavesdropping.

Secured Transfer Of Cipher

The encrypted data is sent to receiver through virtual private network or public network. It is not possible to read the data since it is completely encrypted thrice. If hacker finds hard to read the message.

Triple Security

It provides triple encryption method such enigma computation, time variant random number and transposition& key injection.

5. Conclusions

The key escrow encryption has emerged as one approach that can meet the confidentiality and data recovery needs of organizations while allowing authorized government access to fight terrorism and crime.

It can facilitate the promulgation of standards and products that support the information security requirements of the global information infrastructure. Future work proposed is to implement the Soft Enigma along with the time variant random numbers to encrypt the most Sensitive Data into a successful project for the confidential data maintaining sectors.

References

1. Clifton C and Marks D, Security and privacy implications of data mining in: Proc of ACM SIGMOD, Workshop on Data Mining and Knowledge Discovery, 1996, p.15-19.

2. Verykios V. S, Bertino E, Fovino I. N., Provenza L. P., Saygin Y, and Theodoridis Y, State-of-the-art in privacy preserving data mining in: Proc of ACM SIGMOD, 2004, p.5057.

3. Ackerman, M. S., Cranor, L. F., and Reagle, J, Privacy in ecommerce: examining user scenarios and privacy preferences in: Proc. EC99, 1999, p. 1-8.

4. Sweeney K , k-anonymity: a model for protecting privacy, International Journal on Uncertainty, Fuzziness and Knowledge based Systems, 2002, 10-5 , p. 557-570.

5. VidyaBanu R , Nagaveni N, A Model Based Framework for Privacy Preserving Clustering Using SOM.,International Journal of Computer Applications, 2010, 13 p17-21.

6. VidyaBanu R , Nagaveni N ,Evaluation of a perturbation-based technique for privacy preservation in a multi-party clustering scenario, Information Sciences ,2013,232 p437-448.

7. VidyaBanu , Nagaveni N, Low Dimensional Data Privacy Preservation Using Multi Layer Artificial Neural Network, International Journal of Intelligent Information Technologies ,2013, 8-3, p17-31.

8. Makoto Matsumoto and Takuji Nishimura,Dynamic Creation of Pseudorandom Number Generators, Introduction to Dynamic creation of pseudorandom Number Generator, 2000

9. A. Talha Yalta and Sven Schreiber: Random Number Generation ingretl, Journal of Statistical Software, 2012.

10. Coveyou R R, Random Number Generation Is too Important to Be Left to Chance., Studies in Applied Mathematics , 1969,3- 70, p 111.

11. Coddington P D, Tests of Random Number Generators Using Ising Model Simulations, International Journal of Modern Physics, 1996, 7-295,p 303.

12. McCullough B D, MicrosoftExcel's `Not the Wichmann-Hill' Random Number Gen-erators, Computational Statistics & Data Analysis,2008, 52, P 4587-4593.

13. Vinod H D, Review of GAUSS for Windows, Including Its Numerical Accuracy, Journal of Applied Econometrics, 2007, 15- 211, p. 220.

14. Yalta AT, The Numerical Reliability of GAUSS 8.0."The American Statistician, 2007, 61-262, p 268.

15. ShishirShukla, Prabhat Kumar Verma , Implementation of Affine Substitution Cipher with Keyed Transposition Cipher for Enhancing Data Security , International Journal of Advanced Research in Computer Science and Software Engineering Research Paper,2014, 4-1

16. SukalyanSom, SabyasachiGhosh, A Simple Algebraic Model based Polyalphabetic Substitution Cipher, International Journal of Computer Applications , 2012 ,39 -8 .

17. Sojwal S. Kulkarni ,H.M.Rai , Dr. Sanjay Singla , Effective Substitution Cipher Algorithm for Information Security , International Journal of Innovations in Engineering and Technology , 2012 1- 2 .1

18. MassoudSokouti ,BabakSokouti, SaeidPashazadeh, An approach in improving transposition cipher system,Indian Journal of Science and Technology , 2009, 2- 8 .